CYBER CODEX

Cyber Regulatory Framework Masterclass

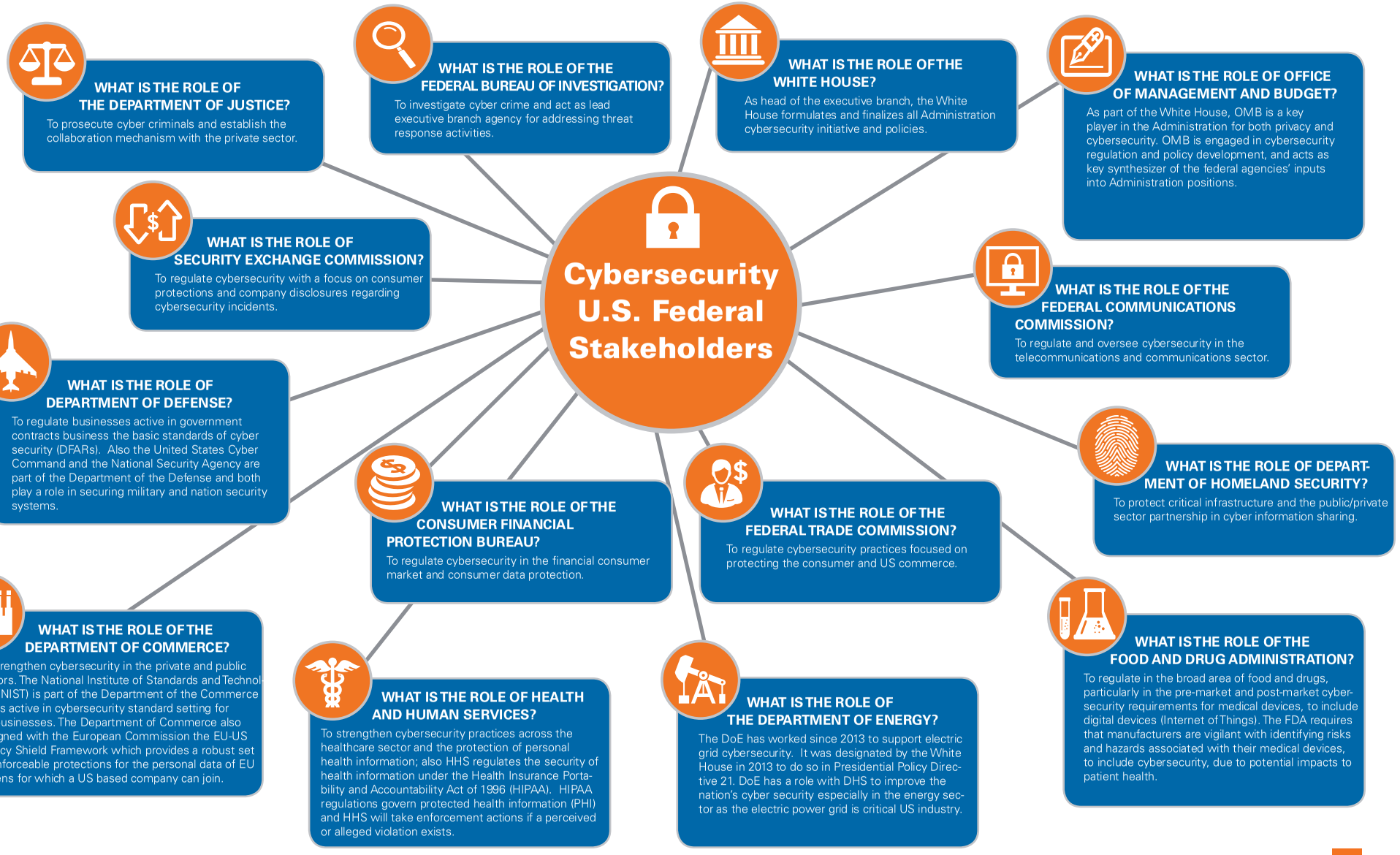
SECTION I	CYBERSECURITY U.S. FEDERAL STAKEHOLDERS
SECTION II	UNITED STATES AND INTERNATIONAL CYBER STANDARDS
SECTION III	CYBERSECURITY LEGAL EXPECTATIONS AND STANDARDS

The Wilson Center thanks its partners for their cybersecurity legal expertise for the content of this publication; Ms. Nancy Sumption, ESQ., for Section I and Ms. Diane M. Janosek ESQ., CISSP, for Sections II and III.

Wilson Center

US FEDERAL REGULATORY AGENCIES

The United States Government Executive Branch is expansive in its efforts to protect the economic security and national security of the nation. Within the Executive Branch, all reporting to the chief of the Executive Branch, the President of the United States, multiple agencies have specific and complementary roles. The Executive Branch, together with the Legislative Branch and the Judicial Branch, work to implement sound cyber security policies.



I

CYBERSECURITY U.S. FEDERAL STAKEHOLDERS

The United States Government Executive Branch is expansive in its efforts to protect the economic security and national security of the nation. Within the Executive Branch, all reporting to the chief of the Executive Branch, the President of the United States, multiple agencies have specific and complementary roles. The Executive Branch, together with the Legislative Branch and the Judicial Branch, works to implement sound cyber security policies.

WHAT IS THE ROLE OF THE WHITE HOUSE?

As head of the Executive Branch, the White House formulates and finalizes all Administration cybersecurity initiative and policies.

WHAT IS THE ROLE OF THE OFFICE OF MANAGEMENT AND BUDGET?

As part of the White House, OMB is a key player in the Administration for both privacy and cybersecurity. OMB is engaged in cybersecurity regulation and policy development, and acts as key synthesizer of the federal agencies' inputs into Administration positions (White House response to legislative proposals).

WHAT IS THE ROLE OF THE DEPARTMENT OF JUSTICE?

To prosecute cyber criminals and establish the collaboration mechanism with the private sector.

WHAT IS THE ROLE OF THE FEDERAL BUREAU OF INVESTIGATION?

To investigate cyber crime and act as the lead in the Executive Branch for addressing cyber threat response activities.

WHAT IS THE ROLE OF THE DEPARTMENT OF COMMERCE?

To strengthen cybersecurity in the private and public sectors. The National Institute of Standards and Technology (NIST) is part of the Department of the Commerce and is active in cybersecurity standard setting for businesses. The Department of Commerce also designed with the European Commission the EU-US Privacy Shield Framework which provides a robust set of enforceable protections for the personal data of EU citizens for which a US based company can join.

WHAT IS THE ROLE OF DEPARTMENT OF HOMELAND SECURITY?

To protect critical infrastructure and the public/private sector partnership in cyber information sharing.

WHAT IS THE ROLE OF THE FEDERAL COMMUNICATIONS COMMISSION?

To regulate and oversee cybersecurity in the telecommunications and communications sector.

WHAT IS THE ROLE OF THE FEDERAL TRADE COMMISSION?

To regulate cybersecurity practices focused on protecting the consumer and US commerce.

WHAT IS THE ROLE OF THE CONSUMER FINANCIAL PROTECTION BUREAU?

To regulate cybersecurity in the financial consumer market and consumer data protection.

WHAT IS THE ROLE OF SECURITY EXCHANGE COMMISSION?

To regulate cybersecurity with a focus on consumer protections and required company disclosures regarding cybersecurity incidents.

WHAT IS THE ROLE OF DEPARTMENT OF DEFENSE?

To regulate businesses active in government contracts by setting the basic standards for cybersecurity management (DFARs). Also the United States Cyber Command and the National Security Agency are part of the Department of the Defense and both play a role in securing military and nation security systems.

WHAT IS THE ROLE OF HEALTH AND HUMAN SERVICES?

To strengthen cybersecurity practices across the healthcare sector and the protection of personal health information. Also HHS regulates the security of health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA regulations govern projected health information (PHI) and HHS will take enforcement actions if a perceived or alleged violation exists.

WHAT IS THE ROLE OF THE FOOD AND DRUG ADMINISTRATION?

To regulate in the broad area of food and drugs, particularly in the pre-market and post-market cybersecurity requirements for medical devices, to include digital devices (Internet of Things). The FDA requires that manufacturers are vigilant with identifying risks and hazards associated with their medical devices, to include cybersecurity, due to potential impacts to patient health.

WHAT IS THE ROLE OF THE DEPARTMENT OF ENERGY?

The DoE has worked since 2013 to support electric grid cybersecurity. It was designated by the White House in 2013 by Presidential Policy Directive 21. DoE has a role with DHS to improve the nation's cybersecurity especially in the energy sector as the electric power grid is critical US industry.

II

UNITED STATES AND INTERNATIONAL CYBER STANDARDS

WHAT IS THE UNITED STATES NIST CYBERSECURITY FRAMEWORK? WHAT STANDARDS ARE PROMOTED?

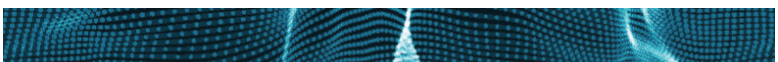
The National Institute of Standards and Technology, part of the United States Department of Commerce, is active in promoting and advocating cybersecurity standards. The agency promotes voluntary compliance so the entire nation can improve its economic security and national security posture. In January 2017, the NIST issued a draft update to its "Framework for Improving Critical Infrastructure Cybersecurity." This updated Framework provides new guidance for entities to help manage cybersecurity risk in areas such as the management of supply chain risk. Overall NIST promotes the Framework so entities can strive to meet common standards and expectations and in turn reduce shared risk, especially in the United States of America where commerce and business partnerships thrive.

Example: NIST first began promoting these voluntary cybersecurity risk standards for American entities operating in the critical infrastructure arena, such as the electric power grid, but now the NIST standards are becoming the expected protocols to conduct business in a digital world. (aka the universal language for cyber risk management)

WHAT IS THE CURRENT FEDERAL ACQUISITION RULE ON CYBERSECURITY REQUIREMENTS FOR COMPANIES CONDUCTING GOVERNMENT BUSINESS?

A new Federal Acquisition Regulation (FAR) contract clause (FAR 52.204-21) became effective in 2016 which imposed a rule on safeguarding contractor information systems, which now standardizes cybersecurity rules for government contractors across agencies. This rule mandates 15 basic safeguarding security controls for contractor information systems upon which Federal contract information transits or resides.

Example: As a subcontractor to a prime government contractor for which government contract information transits, these rules now apply and if not followed, pose a performance risk to the prime contractor and subcontractor.



WHAT IS THE CURRENT DEPARTMENT OF DEFENSE RULE ON CYBERSECURITY REQUIREMENTS FOR BUSINESSES CONDUCTING WITH THE DOD?

The Department of Defense issued a supplement to the Defense Federal Acquisition Regulation (DFARS 252.204-7012). Now Defense contractors, must no later than December 31, 2017, must certify that the contractor's systems are compliant with new reporting requirements. Cleared defense contractors must report penetrations of networks and information systems, and provide DoD personnel access to equipment and relevant information after a computer system compromised may have occurred. DoD can then assess the impact of any potential or actual cyber incident, a compromise, or a penetration.

Example: As a Defense contractor, the business entity must comply with both the FAR and DFARS clauses. Reporting requirements for cyber incidents are more stringent with a higher expectation of cooperation for cyber incidences and compromises.

WHAT ARE THE U.S. CRITICAL SECTORS REGULATED BY THE EXECUTIVE BRANCH?

The United States identified 16 critical infrastructure sectors (in Presidential Policy Directive 21). This designation means that these entities' assets, systems and networks are so vital to the nation's economic security, national security, and public health, that the United States must have a plan in strengthen these critical infrastructure sectors and strive for resiliency.

Example: The 16 critical infrastructure sectors in the United States are:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Sector-Specific Agencies
- Transportation Systems Sector
- Water and Wastewater Systems Sector

IS NEW YORK STATE, THE FINANCIAL CAPITAL OF THE WORLD, REGULATING IN THE CYBERSECURITY ARENA?

Yes. The New York State Department of Financial Services (NYDFS) issued a rule (23 NYCRR 500) establishing cybersecurity standards for financial services institutions. This rule is quite specific with annual certifications required. This rule took effect March 1, 2017. New York enacted the regulation after a series of data breaches at financial institutions and major corporations. A cybersecurity program with periodic risk assessments and a written policy must be in place for New York financial institutions, insurance companies, and financial services firms licensed by the State of New York. These entities must inform the State of any cybersecurity breach within 72 hours.

Example: A satisfactory New York State financial services entity's cybersecurity plan would set forth policies and procedures for the protection of information systems and nonpublic information and address:

- information security;
- data governance and classification;
- asset inventory and device management;
- access controls and identity management;
- business continuity and disaster recovery planning and resources;
- systems operations and availability concerns;
- systems and network security;
- systems and network monitoring;
- systems and application development and quality assurance;
- physical security and environmental controls;
- customer data privacy;
- vendor and third-party service provider management;
- risk assessment; and
- incident response.

WHAT IS THE GDPR?

It is the European Union's General Data Protection Directive (Regulation (EU) 2016/679). The GDPR is intended to strengthen and unify data protection for EU citizens.

Example: The EU has a two-year waiting period for the regulation's effective date, which will be May 25, 2018. There are financial penalties for noncompliance.

WHAT IS THE EU-US SAFE HARBOR AGREEMENT?

EU-US Safe Harbor is an aspect of the EU General Data Protection Directive, which requires that the personal data of EU citizens not be transmitted, even when permitted by the individual, to countries outside if the EU unless the receiving country is perceived by the EU to adequately protect their data. The EU perceives the US to have less stringent protection of personal data. The safe harbor provision provides the framework to authorize data sharing. To be authorized data sharer, US organizations and businesses must voluntarily consent to the data privacy principles in the GDPR.

Example: To enforce an alleged violation of personal data of EU citizens by an American business, the U.S. Department of Commerce is designated by the European Commission to enforce the protections of the EU-US Privacy Shield Framework.

III

CYBERSECURITY LEGAL EXPECTATIONS AND STANDARDS

Multiple federal agencies are now regulating in the area of cybersecurity, and now national stakeholders, stock shareholders and customers all expect business entities to have strong cybersecurity measures in place. The below outlines the expected practices and basic protocols for secure digital transactions *to operate in the United States.*

WHAT STANDARD OF CARE IS EXPECTED WHEN DOING BUSINESS IN CYBERSPACE?

The standard of care is due diligence. A reasonable process must be in place. All employees of the company must adhere to reasonable cybersecurity measures and must know what steps to take based upon variables. The level of a company's security practices must be commensurate with the sensitivity and volume of consumer data to which it has access as well as the complexity of the business operation.

Example: A company must ensure that its staff is able to and does implement "patches" when updates become available to address a known vulnerability in order to protect consumer data.

WHAT ARE THE THREE PRINCIPLES OF CYBERSECURITY THAT GUIDE THE CREATION AND IMPLEMENTATION OF A COMPANY'S PROGRAM?

Confidentiality, Integrity, and Availability

Example: A strong approach to security includes protecting individual data sources and/or data on a network (confidentiality), ensuring the data does not get altered or corrupted (integrity), and ensuring that the data can be accessed and retrieved when needed (availability).

WHAT IS THE FREEZING AN ACCOUNT REQUIREMENT?

This is a mandate to suspend or disable a user's account after multiple unsuccessful login attempts.

Example: Businesses are to implement automatic freezing of account in certain situations. To fail to freeze an account in such situations would put businesses networks at risk, and in turn would place customers' information at risk for exploitation.

WHAT IS THE PROHIBITION ON STORING USER CREDENTIALS IN PLAIN TEXT?

User credentials cannot be stored in clear, readable text.

Example: The Federal Trade Commission can charge companies for failure to store credentials properly, especially for failure to securely store credit card information. To implement proper protection, businesses must have a practice so administrative passwords are not sent in plain text in personal email accounts.

WHAT DOES STORING CREDENTIALS SECURELY MEAN?

Customers' personal data, financial transaction data, and administrative passwords must be encrypted at rest, and must be subject to additional measures, such as two-factor authentication.

Example: To allow one's access to data, two-factor authentication requires two methods to verify one's identity. One method is 'something you have' (i.e. a certificate); another could be 'something you know' (i.e. a password); and a third could be 'something you are' (i.e. a biometric characteristic). Most of us are familiar with two-factor authentication (a card with a chip and entering a PIN). Two-factor authentication means two elements must be met to restore or obtain an updated password (such as providing a specific personal question *and* something specific about the account) for successful verification of credentials.

WHAT IS THE REQUIREMENT TO PROTECT AGAINST AUTHENTICATION BYPASS?

Hackers use known common vulnerabilities and run scripts against a website. Thus, companies must test their web applications for widely-known security flaws to ensure their networks are protected against authentication bypass. The requirement is for companies to use proper cybersecurity due diligence in their digital networks.

Example: Without technical protocols in place, a hacker could predict patterns and bypass the web application's authentication screen and gain authorized access. Widely-known security flaws are often published and companies have an obligation to "patch" the vulnerabilities. In some cases, businesses do not exercise prudent reviews and fail to patch. Hackers know this, and exploit them, by trying multiple websites with a similar hacking method to exploit the widely-known security flaws.

WHY ARE US COMPANIES ADOPTING SECURE REMOTE ACCESS MORE FREQUENTLY?

With the rise of telecommuting, mobility, and the demand to access work files ubiquitously, companies are implementing more secure remote accesses for their employees. Secure remote access also leaves confidential, personal privileged and/or proprietary data on a company's home network (versus an employee's home laptop or mobile device). This approach is one demonstration of a company's due diligence and a commitment to cybersecurity best practices.

Example: Secure remote access today is generally through use of a VPN, SSH, or SSL tunnel.

WHAT ARE THREE AREAS IN WHICH BUSINESSES NEED TO INVEST TO LIMIT UNAUTHORIZED ACCESS TO PROPRIETARY AND PERSONAL DATA BY BOTH OUTSIDERS (NON-EMPLOYEES) AND INSIDERS (EMPLOYEES)?

Administrative, Technical, and Physical Access Controls. Administrative controls are internal company processes or training, which are understood and implemented by all employees. Technical controls are protocols that automatically occur through software, hardware or firmware triggering mechanisms. Physical access controls are items that permit physical access to data only when necessary for performance of duties.

Examples: Administrative controls include keeping current standard operating procedures in place and training employees whenever updates occur (but no less than once a year). Technical controls include automatic freezing of account after unsuccessful multiple logins attempts, as well as encryption and firewalls. Physical access controls include both people (security guards) and objects (uniquely locked doors to data center or hard drives). These three consistent business practices, used together, demonstrate due diligence and layered defense in a cybersecurity program.